ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 7, July 2016

Communication Security Enhancement in Wireless Sensor Networks - An Application of RSA algorithm

Harmanjot Kaur, Paramjit Singh

***Abstract*- Wireless sensor devices are used in many application areas. Security is a vital context for such networks also. Security goals like confidentiality, integrity, data origin authentication, access control and availability are set. Cryptography is used to secure the communication data packets. It encrypts the data while transmitting it and decrypts it back at the receiver end. Today, various cryptography techniques and algorithms exist. Cryptography algorithms are complex, slow, power hungry. They involve high computations and require more processing power which makes them impractical for the wireless network nodes. RSA with 512 bit key length is used for encryption and decryption data. Even breaking into this level of security is not easy. As these devices have low computation power, small memory and battery power, very complex algorithms cannot be used. In this thesis in order to enhance the network security and make the communication more secure, RSA with 1024-bit and 2048-bit key length and 4096-bit key length has been used to enhance the communication security. Doing encryption and decryption on test files we compare the results on time and power consumption**.

Keywords: **Encryption, Decryption, RSA, WSN.**

I. INTRODUCTION

In the today's computing world, fast communication which must be secure is the need of the hour. Various networks are joined together in Internet to form the world a global village. Distributed networks have become the backbone for providing online transactions and other services. Wireless sensor networks are an important part of the communications world. Taking into consideration, the various characteristics of the Wireless Sensor Networks there is a need of new techniques to provide security and integrity.

Security in data communication in the Wireless Sensor Network is the aim of the present paper. Asymmetric approach of cryptography using the RSA algorithm is used to protect the network information and resources from the unauthorized access. Including the wireless networking, all the data communication over the network requires security. Taking the case of wireless sensor networks, there are various constraints in providing high level of security using complex algorithm. Various constraints in the WSN include low computation capability, small memory, limited energy resources[3], susceptibility to physical capture, lack of infrastructure. These issues put security challenges and require making innovative approaches desirable.

II. SECURITY THREATS AND CONSTRAINTS

Various threats are present that challenge the network security of the wireless sensor networks. From the various threats, major security threats are the attacks like DoS (Denial of Service) Attack, Node Clone Attack and Sybil Attack, Sinkhole Attack, Wormhole Attack, Hello Flood Attacks etc. These threats make the network no responsive or extremely slow so that no services can be provided and on the other side, these attacks capture the network traffic by becoming false nodes and thus try compromise the network security[32].

In the wireless nodes, batteries are the source of energy. So, while providing security using existing security mechanisms are inadequate because energy consumption becomes a key consideration and new approaches are desired.

III. Cryptography

Cryptography helps to secure the data communication over the network. Cryptography is used to encrypt the data at the transmission end and decrypt it back at the receiving end. Today, there are many cryptography techniques and algorithms available. But we can not implement any algorithm as they are exist but these cryptography algorithms are complex, slow and power hungry. They require more processing power because of high computations involved which make them impractical for the low power battery operated wireless network nodes. Cryptography has four basic goals known as Confidentiality, Integrity, Authentication and No repudiation. Based on the number of keys involved in the encryption and decryption process, there are three types of algorithms that are employed[7], and further defined by their application and use.

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

A) Symmetric Cryptography Algorithms

Symmetric cryptography algorithms include Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption Algorithm (IDEA), Blowfish, Skipjack, Advanced Encryption, and Standard (AES). Various limitations of Symmetric Algorithms[6] are distribution of the key is the problem, because once the key is compromised, it

means a total security leak. It does not provide No repudiation of data. Once a member of a security group leaves a new key must be generated and distributed.

B) Asymmetric Key Algorithms

These algorithms use two keys - public and private which are used for data encryption and data decryption. One of the keys is the Public key that is shared to all whereas each member of the group had his own private key, which is private to him and only known to him. The public key algorithms cover up all the weakness found in symmetric key system. Examples of Asymmetric Key algorithms are Diffie-Hellman, RSA, Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC) are currently in use. The most commonly used asymmetric algorithm is the RSA algorithm.

C) Hashing Algorithms

Hashing algorithms are the most secure of all three. These are used with digital signatures, it provides a fixed length digital digest of a message and it is almost impossible to derive a message from its hash function. Also it is very much unlikely that the same two messages will generate the same hash function and so it is considered as a very effective way to ensure security and integrity of the message transmitted. Examples of Hash algorithms are Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5), Secure Hash Algorithm (SHA), Hash-Based Message Authentication Code (HMAC).

IV. RSA ALGORITHM

The popular RSA algorithm invented in 1977 is named after Ron Rivest, Adi Shamir and Len Adleman[11]. Although the basic technique was first discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997 and also, the patent taken out by RSA Labs has expired. The RSA algorithm can be used for both public key encryption and digital signatures. The security is based on the difficulty of factoring large integers in the algorithm. RSA-512 key length which was wide spread is not considered any more. The requirement of more security made to think about the solution to provide security in the data communication over the network.

Although 512-bit RSA keys protect approximately 95% of today's E-commerce on the Internet at least outside the USA and are used in SSL (Secure Socket Layer) handshake protocols till 2010. Understanding the urgency of the undesirable situation, it became important to use “strong" cryptography by increasing the RSA key length. As a result, the work was done to enhance the security and use larger key length by replacing the 512-bit keys by 768-bit.

This was thought that this will create the much more favorable conditions for secure internet communication. But it too was unable to provide the required level of security. So the need to implement RSA-1024 bit becomes necessary to cope up with the upcoming needs for security[15]. Now, with enhancement in technology, RSA-2048 and RSA-4096 bit key length is the need of the hour which is used in the present work to see the viability and the security level in the wireless sensor network.

A) RSA Hardware - The New Trend

There are various constraints for larger key lengths. Wireless Sensor network nodes are low power battery operated devices. Recharging of the battery is also not feasible. The processing power of the sensor nodes is also less. So, deploying the high computation algorithm also becomes less feasible. Also, the memory constraint is also there and so the memory available for computations is also less. These constraints restricted the implementation in the previous years.

The new trends in the RSA algorithm implementation is RSA Hardware. This is a specialized hardware that is plugged in the form of boxes and added to the communication line that encrypts the communication data at the source end and decrypts the data back at the receiving end. This hardware is becoming the ultimate choice for the high security as well as military applications. The major benefit of using RSA hardware is that it does not put any load on the main processor. These boxes have independent memory and battery power.

There is a separate processor dedicated for the encryption purpose. Moving encryption work to other processor will make the whole system faster. Also, the RSA hardware is considered as more secure as compared to the software algorithm implementation. The software implementation has no physical security whereas hardware encryption boxes are tamper proof and prevent someone from modifying a hardware encryption device. Also, RSA Hardware needs considerably less power and time as compared to the RSA software and is easy to implement and secure[32].

B) RSA Key length

The key length of an RSA key, it is basically referring to the length of the modulus, *n*, in bit[10]. A key length of 768 bits or 1024 bits is now no longer considered secure. The longer the information is needed to be kept secure, the longer the key you should use. Keep up to date with the latest recommendations in the security journals.

V. COMPARATIVE STUDY

Presently, RSA is being used in the network security with 1024 bits key length. This RSA-1024 is accepted level of security for the network. The following section covers the comparative study of different key lengths with respect to their encrypting and decrypting time as well as energy consumed by each by taking 240 kb of input data size.

RSA with 2048-bit keys (RSA-2048) and 4096-bit keys (RSA-4096) is implemented which provides a currently accepted level of security for many applications to protect data beyond the encryption of a 1024-bit block[12].

A) Encrypting Data

The original message (plaintext) is encrypted and converted into the cipher text. Results show the comparison of RSA-512, RSA-1024, RSA-2048 and RSA-4096. It is done on the basis of some parameters like time and energy consumption.

Encryption

Sender A does the following:-

- Obtains the recipient B's public key (n, e).

- Represents the plaintext message as a positive integer *m*.

Computes the ciphertext $c = m^e \bmod n$.

- Sends the ciphertext *c* to B.

After analyzing this time by taking different data sizes, the average time consumed is 742.23 ml sec for RSA 1024 and for RSA 2048, its is 663.30 ml sec whereas for RSA-4096 is 612.15 ml sec.

Table (a) Encryption Times with Various File Size

	Encryption times			
File Size (Kb)	**512**	**1024**	**2048**	**4096**
18 kb	54	45	38	32
69 kb	73	61	55	45
138 kb	102	78	64	54
275 kb	134	106	82	67
549 kb	158	135	112	85
886 kb	194	175	148	132
1097 kb	252	225	198	176
6582 kb	310	274	235	219
7015 kb	624	523	487	412
9872 kb	1517	1342	1240	1103
19744 kb	1934	1765	1523	1378
39488 kb	2703	2345	2154	2087
69104 kb	3026	2575	2287	2168
Average	**852.4**	**742.2**	**663.3**	**612.2**

B) Decrypting Data

Decryption

Recipient B does the following:-

- Uses his private key (n, d) to compute $m = c^d \bmod n$.
- Extracts the plaintext from the message representative *m*.

Results shows that when the decryption is done then 4096 is taking more time then 2048 & 1024 bits to decrypt the data. This makes this algorithm more time consuming and therefore, overhead is also increased.

After analyzing this time by taking different data sizes, the average time consumed is 22.92 ml sec for RSA 1024 and for RSA 2048 , its is 171.23 ml sec and for RSA-4096 it is 1025.53 ml sec.

Table (b) Decryption Times with Various File Size

	Decryption times			
File Size (Kb)	**512**	**1024**	**2048**	**4096**
18 kb	4	6	18	34
69 kb	5	8	23	67
138 kb	6	11	37	102
275 kb	7	13	56	167
549 kb	8	15	73	223
886 kb	9	17	97	312
1097 kb	11	20	123	526
6582 kb	13	24	166	822
7015 kb	15	27	207	1213
9872 kb	17	33	263	1721
19744 kb	20	36	331	2246
39488 kb	22	42	392	2703
69104 kb	25	46	440	3195
Average	**12.5**	**22.9**	**171.2**	**1025.5**

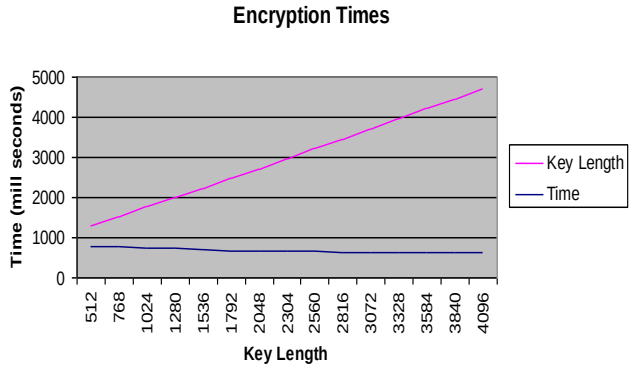

Figure 'a' *RSA encryption time by key length*

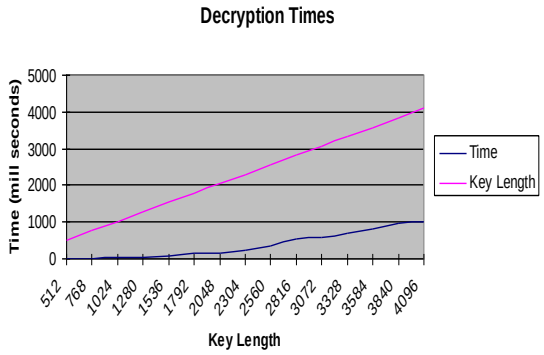

Figure 'b' *RSA decryption time by key length*

VI. CONCLUSION

Cryptography is used to secure the communication data packets. It encrypts the data while transmitting it and decrypts it back at the receiver end. Today, various cryptography techniques and algorithms exist. Cryptography algorithms are complex, slow, power hungry. They involve high computations and require more processing power which makes them impractical for the wireless network nodes.

RSA with 4096-bit keys (RSA-4096) is able to secure the network communication data and is possible to implement in the wireless sensor nodes. It provides much secure level of level of security for many applications to protect data beyond the encryption of a 4096-bit block.

VII. FUTURE SCOPE

We are heading towards a future of miniaturization and wireless connectivity and sensor networks have the ability to deliver both at very low cost. For future research we propose extending this security framework to include trust establishment and trust management in sensor networks. Besides this we have an interest in exploring and solving security issues in multimedia and biometric security, cyber security and information assurance, protection against identity theft, and forensic computing. To address these unique security concerns, it would be imperative to study the adjacent technological advances in distributed systems, ubiquitous computing, broadband wireless communication, nanofabrication and bio-systems. Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. Firstly, the security mechanisms are highly application-specific so the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes. Secondly, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints.

REFERENCES

[1.] S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53{57, 2004}.

[2.] Agah, S. K. Das, K. Basu, and M. Asadi. Intrusion Detection in Sensor Networks: a Non-Cooperative Game Approach. In Proceedings of Third IEEE International Symposium on the Network Computing and Applications (NCA'04), pages 343 – 346. IEEE Computer Society, 2004.

[3.] Bekara and M. Laurent-Maknavicius. A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), pages 59–59, 2007.

[4.] Bertoni, L. Breveglieri, and M. Venturi. ECC Hardware Coprocessors for 8-bit Systems and Power Consumption Considerations. In Third International Conference on Information Technology: New Generations (ITNG 2006), pages 573–574, 20

[5.] Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation, 164(1):1–23, 1998.

[6.] Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.[Online]. Available:

[7.] Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[8.] D. Chakrabarti, S. Maitra, and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In Information Security, pages 89– 103. LNCS 3650, 2005.

[9.] Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 2004, pp. 162-175.

[10.] Lin and G. Noubir, "Low Power DOS Attacks in Data Wireless LANs and Countermeasures," Northeastern University, Tech. Rep., 2002. [Online].

[11.] R. Anderson, H. Chan, and A. Perrig. Key Infection : Smart Trust for Smart Dust. In Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04), pages 206–215, 2004.

[12.] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir. On the Detection of Clones in Sensor Networks Using Random Key Predistribution. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37(6):1246–1258, 2007.

[13.] S. S. C¸amtepe and B. Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 15(2):346–358, 2007.

[14.] Stefania Cavallar , "Factorization of a 512-bit RSA Modulus" CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands, fcavallar,walter,hermang@cwi.nl
[15.] T. Arampatzis, J. Lygeros, and S. Manesis. A Survey of Applications of Wireless Sensors and Wireless Sensor Networks. In Proceedings of the 13th Mediterranean Conference on Control and Automation, pages 719–724, 2005.
[16.] Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-7, Feb. 2004.

[17.] Abdul D S, Elminaam, Kader H M A and Hadhoud M M (2008), "Performance Evaluation of Symmetric Encryption Algorithms," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December.
[18.] Anjum F, Subhadrabandhu D and Sarkar S (2004), "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols", In IEEE 58th Vehicular Technology Conference.
[19.] Dhawan P (2002), "Performance Comparison: Security Design Choices," Microsoft Developer Network October.
[20.] Minaam D S A, Kader H M A, and Hadhoud M M (2010), "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, Vol.11, No.2, PP.78–87, Sept.
[21.] Uddin M, Khowaja K and Rehman A A (2010), "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October.
[22.] Sen J (2010)," An intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks", Second International Conference on Computational Intelligence, Communication Systems and Networks.
[23.] Schneier B (1996), "Applied Cryptography", John Wiley and Sons, Inc.
[24.] Singh B (2006), "Network Security and Management" PHI, New Delhi
[25.] Stallings W (2005), "Cryptography and Network Security, Principles and Practices" Pearson Education, New Delhi
[26.] " Rsa-Based Digital Image Encryption Algorithm In Wireless Sensor Networks" Gaochang Zhao, Xiaolin Yang, Bin Zhou, Wei Wei University of Science and Technology, Chengdu 610065

[27.] " A Survey on Wireless Sensor Network Security" Jaydip Sen, Tata Consultancy Services Limited, Wireless & Multimedia Innovation Lab, Bengal Intelligent Park, Salt Lake Electronics Complex, Kolkata 700091, India

[28.] "Network Security Protocols for Wireless Sensor Networks-A Survey" Pritam Gajkumar Shah Lecturer, Telecom Engineering Department RV College of Engineering, Bangalore

[29.] "Secure Wireless Sensor Networks: Problems and Solutions" Fei Hu, IEEE Member, Computer Engineering Department, Rochester Institute of Technology, Rochester, New York 14623, USA; Jim Ziobro, IEEE Senior Member, Computer Engineering Department, Rochester Institute of Technology, Rochester, New York 14623, USA Jason Tillett, Senior Researcher, Laboratory for Autonomous Cooperative Microsystems College of Engineering, RIT; Neeraj K. Sharma, IEEE Senior Member, Electrical & Computer Engineering Department, Clarkson University, Potsdam, New York 13699, USA;
[30.] "Key Generation Research of RSA Public Cryptosystem and Matlab Implement" Hongjun WANGl, Zhiwen SONG2, Xiaoyu NIUl, Qun DINGl 1 Electronic Engineering College Heilongjiang University, Harbin, China qunding@yahoo.cn yyxzLlove@126.com Quality Inspection Department Harbin Boiler Company, Harbin, China 13614511154@163.com
[31.] "Key Management Schemes of Wireless Sensor Networks : A Survey", SyedMuhammad Khalid-ur-Rahman Raazi, Zeeshan Prevez and Sungyoung Lee, Dept. of Computer Engineering, Kyung Hee University, Global Campus, Korea.
[32.] "Comparison between RSA Hardware and Software Implementation for WSNs Security Schemes", Abdullah Said Alkalbani, Teddy Mantoro, Abu Osman Md Tap, Department of Computer Science, Kulliyyah (Faculty) of Information & Communication Technology.